Commonwealth Office of Technology
Monthly Cyber Security Tips

March 2009   Volume 4, Issue 3

Social Networking Sites: How To Stay Safe

From COT's Chief Information Security Office

The popularity of social networking sites--such as MySpace, Facebook, Twitter and others--has exploded in recent years, with usage in the United States increasing 93% since 2006, according to Netpop Research. The sites are popular not only with teenagers, but with adults as well: the number of adult Internet users having a social networking profile has more than quadrupled in the past four years, according the Pew Internet & American Life Project.

While there are many positive aspects of using social networking sites, it is also important to understand the potential security risks and know what precautions to take to protect yourself and your information.

What are social networking sites?

Social networking sites are online communities of Internet users who want to communicate with other users about areas of mutual interest, whether from a personal, business or academic perspective. The specific functionality of the various sites may differ, but in general, the sites allow you to provide information about yourself and communicate with others through email, chat rooms and other forums.

What are the security concerns of social networking sites?

Social network sites are growing in popularity as attack vectors because of the volume of users and the amount of personal information that is posted. The nature of social networking sites encourages you to post personal information. Because of the perceived anonymity and false sense of security of the Internet, users may provide more information about themselves and their life online than they would to a stranger in person.

The information you post online could be used by those with malicious intent to conduct social engineering scams and attempt to steal your identity or access your financial data. In addition, the sites are increasingly sources of worms, viruses and other malicious code. You may be prompted to click on a video on someone's page, which could bring you to a malicious website, for example. If you are accessing a site that has malicious code your machine could become infected. For examples of some common social networking scams, visit the Council of Better Business Bureaus.

It's also important to realize that information you post can be viewed by a broad audience, and could have lasting implications. College admissions officers and school administrators, for example, do visit these sites and in some cases, admissions have been denied to applicants, or disciplinary actions have been taken because of information or photos posted online. Employers also review these sites for information about potential job applicants.

What can you do to protect yourself?

- **Make sure your computer is protected before visiting sites** – make sure you have a firewall and anti-virus software on your computer and that it is up-to-date. Keep your operating system up-to-date as well.
- **Do not assume you are in a trusted environment** – just because you are on someone's page you know, it is still prudent to use caution when navigating pages and clicking on links or photos, because links, images or other content contained on the pages may include malicious code.
- **Be cautious in how much personal information you provide** - remember that the more information you post, the easier it may be for an attacker to use that information to steal your identity or access your data.
- **Use common sense when communicating with users you DO know** – confirm electronic requests for loans or donations from your social networking friends and associates. The communications could be from someone who has stolen the credentials of the person you know with the intent of scamming as many people as possible.
- **Use common sense when communicating with users you DON'T know –** be cautious about whom you allow to contact you or how much and what type of information you share with strangers online.
- **Understand what information is collected and shared –** pay attention to the policies and terms of the sites; they may be sharing your email address or other details with other companies.
- **Make sure you know what sites your child is visiting -** be involved in your child's activities and know with whom he/she is communicating and what information is being posted by them, or about them by others.

Remember, cyber security is everyone's responsibility. Don't be the weak link in the chain.

Online Resources

To learn more about protecting information visit the following online resources:

- **MS ISAC Monthly Cyber Security Tips**: www.msisac.org/awareness/news
- **US CERT**: www.us-cert.gov/reading_room
- **OnGuard Online**: www.onguardonline.gov/topics.html
- **Privacy Rights Clearinghouse**: www.privacyrights.org

For more cyber security monthly tips go to:
www.msisac.org/awareness/news/
technology.ky.gov/security/CyberAwareness.htm

Brought to you by:

www.msisac.org

technology.ky.gov